

1807.0924

#6
PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:)	
	:	Examiner: Unassigned
Ioana DONESCU)	
	:	Group Art Unit: Unassigned
Appln. No.: Unassigned)	
	:	
Filed: Concurrently herewith)	
	:	
For: METHOD AND DEVICE FOR)	July 7, 1999
INSERTING AND DECODING	:	
A WATERMARK IN DIGITAL)	
DATA	:	



The Assistant Commissioner of Patents
Washington, D.C. 20231

CLAIM TO PRIORITY

Sir:

Applicant hereby claims priority under the International Convention and all rights to which he is entitled under 35 U.S.C. § 119 based upon the following French Patent Applications:

9810148 filed on August 6, 1998; and

9810149 filed on August 6, 1998.

A certified copy of the priority document 9810148 is enclosed. A certified copy of the other priority application, will be submitted separately.

This Page Blank (uspto)

Applicant's undersigned attorney may be reached in our Washington, D.C. office by telephone at (202) 347-8100. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,


Attorney for Applicant

Registration No. 36,570

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

F506\W186154\BLK\vjw

This Page Blank (uspto)



CERTIFIED COPY OF
UTILITY DOCUMENT



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 24 JUIN 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

This Page Blank (uspto)

REQUÊTE EN DÉLIVRANCE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES **06.04.1998**
N° D'ENREGISTREMENT NATIONAL **98 10148 -**
DÉPARTEMENT DE DÉPÔT **75**
DATE DE DÉPÔT **06/08/98**

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE
À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE
RINUY, SANTARELLI
14, avenue de la Grande Armée
75017 PARIS

n° du pouvoir permanent **BIF022028/FR/EP** références du correspondant **01 40 55 43 43** téléphone

2 DEMANDE Nature du titre de propriété industrielle
☒ brevet d'invention ☐ demande divisionnaire
☐ certificat d'utilité ☐ transformation d'une demande de brevet européen
demande initiale ☐ brevet d'invention ☐ certificat d'utilité n°
Établissement du rapport de recherche ☐ différé ☒ immédiat
Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☐ non
Titre de l'invention (200 caractères maximum)
Procédé et dispositif d'insertion et de décodage d'une marque dans des données numériques.

3 DEMANDEUR (S) n° SIREN code APE-NAF
Nom et prénoms (souligner le nom patronymique) ou dénomination
CANON KABUSHIKI KAISHA
Forme juridique
Société de droit Japonais
Nationalité (s) **JAPONAISE**
Adresse (s) complète (s)
30-2, Shimomaruko 3-chome, Ohta-ku, Tokyo, JAPON
Pays
JAPON

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt : joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE
pays d'origine numéro date de dépôt nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE
(nom et qualité du signataire - n° d'inscription)
Bruno QUANTIN N° 2.1206
RINUY, SANTARELLI
SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

DÉSIGNATION DE L'INVENTEUR

(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

BIF022028/FR/EP

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Petersbourg

75800 Paris Cédex 08

Tél. : 01 53 04 53 04 - Télécopie : 01 42 93 59 30

N° D'ENREGISTREMENT NATIONAL

98 10148

TITRE DE L'INVENTION :

Procédé et dispositif d'insertion et de décodage d'une marque dans des données numériques.

LE(S) SOUSSIGNÉ(S)

Société de droit Japonais CANON KABUSHIKI KAISHA

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse et souligner le nom patronymique) :

DONESCU Ioana

37, rue de la Gare

22000 SAINT BRIEUC - France

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

6 août 1998

Bruno QUANTIN N° 92.1206
RINUY, SANTARELLI

5

10 La présente invention concerne un procédé et un dispositif d'insertion d'une information supplémentaire, telle qu'une marque secrète, dans des données numériques.

Elle concerne également un procédé et dispositif de décodage d'une telle information supplémentaire dans des données numériques marquées.

15 Elle s'inscrit de manière générale dans le domaine technique du marquage (en anglais watermarking) des données numériques.

La prolifération des échanges de données multimédia numérisées par voie informatique favorise la création et la distribution de copies illicites, et d'une façon générale, la manipulation illégale de ces données.

20 Le marquage des données numériques consiste à insérer une marque directement dans les données numérisées. L'insertion de cette marque est assimilée au codage d'une information supplémentaire dans les données numériques.

25 Un marquage classique consiste à insérer un logo visible lorsque les données numériques sont des images. Néanmoins, cette marque est facile à enlever pour un utilisateur qui souhaite manipuler illégalement cette image.

On utilise alors fréquemment une marque dite invisible qui doit présenter les facteurs de qualité suivants :

30 Cette marque doit être imperceptible, c'est-à-dire que l'insertion d'une telle marque doit préserver la qualité perceptuelle des données numériques, par exemple, la qualité visuelle pour des images ou la qualité

auditive pour des données audio. L'imperceptibilité de la marque rend en outre son piratage plus difficile.

Cette marque doit également être indélébile, c'est-à-dire être statistiquement indétectable dans les données numériques marquées afin de
 5 résister aux attaques intentionnelles pour détruire cette marque.

Cette marque doit en outre être robuste aux traitements classiques appliqués aux données numériques, tels que compression et décompression, transformation numérique / analogique, filtrage...

Cette marque doit enfin être fiable, c'est-à-dire permettre une
 10 décision fiable quant à l'existence ou non d'une marque donnée dans des données numériques données.

On connaît un procédé d'insertion d'une marque, décrit dans la Demande de Brevet européen N° 0 766 468 au nom de NEC CORPORATION, dans lequel on réalise une transformation fréquentielle des données
 15 numériques avant d'insérer l'information supplémentaire dans des composantes significatives perceptuellement. Une transformation fréquentielle inverse permet d'obtenir les données numériques marquées. De préférence, une transformée en cosinus discrète est appliquée sur l'ensemble des données numériques, par exemple une image, et on module les N plus grandes composantes
 20 fréquentielles, en excluant la composante continue qui représente la plus basse fréquence de l'image, pour insérer l'information supplémentaire.

La présente invention a pour but principalement d'améliorer ce procédé d'insertion et d'accroître la qualité de la marque insérée, notamment en terme d'imperceptibilité et de robustesse.

25 Conformément à l'invention, le procédé d'insertion d'une information supplémentaire, telle qu'une marque secrète, dans des données numériques, est caractérisé en ce qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution des données numériques ;
- 30 - extraction des composantes d'une sous-bande de fréquences ;
- transformation spectrale des composantes de ladite sous-bande de fréquences ;

- choix d'un sous-ensemble de coefficients de ladite transformation spectrale ;

- modulation des coefficients dudit sous-ensemble pour insérer l'information supplémentaire ;

5 - transformation spectrale inverse des coefficients incluant le sous-ensemble de coefficients modulés ; et

- recomposition spectrale multi-résolution inverse des données numériques marquées.

10 Corrélativement, un dispositif d'insertion d'une information supplémentaire, telle qu'une marque secrète, dans des données numériques, est caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution des données numériques ;

15 - des moyens d'extraction adaptés à extraire des composantes d'une sous-bande de fréquences ;

- des moyens de transformation spectrale des composantes de ladite sous-bande de fréquences ;

- des moyens de choix pour choisir un sous-ensemble de coefficients de ladite transformation spectrale ;

20 - des moyens de modulation des coefficients dudit sous-ensemble pour insérer l'information supplémentaire ;

- des moyens de transformation spectrale inverse des coefficients incluant le sous-ensemble de coefficients modulés ; et

25 - des moyens de recomposition spectrale multi-résolution inverse des données numériques marquées.

Grâce à cette double transformation des données numériques, la recherche des coefficients à moduler est mise en œuvre sur un domaine limité de fréquences. En effet, un choix préalable est réalisé à travers la décomposition spectrale multi-résolution, ce qui permet de localiser les coefficients modulables de façon automatique dans une zone du spectre, et non dans tout le domaine spectral. Ceci est particulièrement bien adapté à la

30

vérification de la marque insérée, par exemple lorsqu'il s'agit de vérifier des droits d'auteur sur une image numérisée.

En outre, le choix préalable d'une bande de fréquences modulable permet de sélectionner de manière systématique des composantes
5 fréquentielles robustes à divers algorithmes de compression des données numériques.

Enfin, l'application d'une transformation spectrale sur les composantes de la sous-bande choisie garantit une répartition de l'information supplémentaire insérée ultérieurement sur tout le domaine spatial des données
10 numériques. En outre, cette transformation spectrale est réalisée sur une sous-bande des données numériques initiales, de taille plus petite. La transformation spectrale est donc beaucoup plus rapide que dans les procédés connus dans lesquels la transformation spectrale est effectuée sur l'ensemble des données numériques initiales.

15 Selon une version préférée de l'invention, à l'étape d'extraction, on choisit les composantes de la sous-bande de plus basse fréquence.

Ce choix est particulièrement judicieux lorsqu'il s'agit d'image numérisée afin d'insérer ultérieurement l'information supplémentaire dans un domaine spectral robuste aux méthodes classiques de compression et
20 décompression.

Selon une version avantageuse, particulièrement bien adaptée à l'insertion d'une marque dans une image numérique, à l'étape de décomposition spectrale, la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction, on choisit les composantes de la
25 sous-bande d'approximation.

La Demanderesse a montré, alors qu'il est couramment admis que la sous-bande d'approximation, correspondant aux plus basses fréquences, n'admet que de très faibles modifications sans distorsions visuelles importantes sur l'image reconstruite, qu'il est possible d'ajouter une information
30 supplémentaire sur les composantes de la sous-bande d'approximation de manière imperceptible à condition d'atteindre un niveau de résolution suffisamment faible lors de la décomposition spectrale multi-résolution.

De préférence, le niveau de décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre de composantes de la sous-bande d'approximation est compris entre 8×8 et 32×32 .

La Demanderesse a montré de manière empirique qu'une sous-bande de cette taille convenait particulièrement bien à l'insertion d'une information supplémentaire tout en garantissant l'imperceptibilité de cette information supplémentaire.

Selon une version préférée de l'invention, la transformation spectrale est une transformée en cosinus discrète.

L'utilisation d'une telle transformation spectrale est particulièrement bien adaptée à l'insertion d'une marque dans une image et garantit une bonne répartition dans tout le domaine spatial de la marque insérée.

Selon une version préférée de l'invention, à l'étape de modulation, les coefficients dudit sous-ensemble sont modulés par addition d'une valeur de modulation générée par une fonction pseudo aléatoire initialisée par un signal numérique représentatif de l'information supplémentaire à insérer.

L'addition de l'information supplémentaire au moyen de valeurs de modulation générées par une fonction pseudo aléatoire permet de masquer cette information et de renforcer son invisibilité afin de rendre le piratage de cette information plus difficile.

Selon une version avantageuse de l'invention, à l'étape de choix, le sous-ensemble de coefficients est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique représentatif d'une clé confidentielle associée à l'information supplémentaire à insérer.

Cette clé confidentielle permet de choisir les coefficients modulables de manière pseudo aléatoire et de rendre ainsi l'information insérée plus robuste aux attaques intentionnelles, en rendant sa localisation dans le spectre de fréquence plus difficilement repérable.

Selon une version préférée de l'invention, qui permet une réalisation pratique et commode du procédé d'insertion conforme à l'invention, les moyens de décomposition spectrale, d'extraction, de transformation

spectrale, de choix, de modulation, de transformation spectrale inverse et de recomposition spectrale du dispositif d'insertion sont incorporés dans :

- un microprocesseur,
- une mémoire morte comportant un programme pour insérer une
- 5 information supplémentaire, et
- une mémoire vive comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Un moyen de stockage d'information, lisible par un ordinateur ou par un microprocesseur, intégré ou non au dispositif, éventuellement amovible,

- 10 mémorise un programme mettant en œuvre le procédé d'insertion d'une information supplémentaire conforme à l'invention.

En association avec ce procédé d'insertion, la présente invention vise également un procédé de décodage dans des données numériques marquées d'une information supplémentaire, telle qu'une marque secrète,

- 15 insérée dans des données numériques initiales suivant ledit procédé d'insertion, caractérisé en ce qu'il comporte les étapes suivantes :

- décomposition spectrale multi-résolution des données numériques marquées et des données numériques initiales ;
- extraction des composantes d'une sous-bande de fréquences
- 20 respectivement dans les données numériques marquées et initiales ;
- transformation spectrale des composantes de la sous-bande de fréquence des données numériques marquées et des données numériques initiales ;
- sélection du sous-ensemble de coefficients choisi à l'étape de
- 25 choix dudit procédé d'insertion dans les données numériques marquées et les données numériques initiales ;
- estimation, par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées et des coefficients dudit sous-ensemble des données numériques initiales, d'une séquence estimée de
- 30 valeurs de modulation ;
- génération d'une séquence présumée de valeurs de modulation insérées à l'étape de modulation dudit procédé d'insertion ;

- calcul d'une mesure de corrélation entre la séquence estimée et la séquence présumée ; et

- décision de la similitude ou non de la séquence estimée et de la séquence présumée en fonction de ladite mesure de corrélation.

5 Corrélativement, un dispositif de décodage dans des données numériques marquées d'une information supplémentaire, telle qu'une marque secrète, insérée dans des données numériques initiales suivant le procédé d'insertion conforme à l'invention est caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution des données numériques marquées et des données numériques initiales ;

- des moyens d'extraction des composantes d'une sous-bande de fréquences respectivement dans les données numériques marquées et initiales ;

15 - des moyens de transformation spectrale des composantes de la sous-bande de fréquence des données numériques marquées et des données numériques initiales ;

- des moyens de sélection du sous-ensemble de coefficients choisis à l'étape de choix dudit procédé d'insertion dans les données numériques marquées et les données numériques initiales ;

20 - des moyens d'estimation, par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées et des coefficients dudit sous-ensemble des données numériques initiales, d'une séquence estimée de valeurs de modulation ;

25 - des moyens de génération d'une séquence présumée de valeurs de modulation insérées à l'étape de modulation dudit procédé d'insertion ;

- des moyens de calcul d'une mesure de corrélation entre la séquence estimée et la séquence présumée ; et

30 - des moyens de décision de la similitude ou non de la séquence estimée et de la séquence présumée en fonction de ladite mesure de corrélation.

Grâce à la double transformation des données numériques, la recherche des coefficients modulés est mise en œuvre sur un domaine limité de fréquences. En effet, le choix préalable réalisé à travers la décomposition spectrale multi-résolution permet de localiser les coefficients modulables de façon automatique dans une zone du spectre.

Ce procédé et dispositif de décodage sont particulièrement bien adaptés à la vérification de la marque insérée, par exemple lorsqu'il s'agit de vérifier des droits d'auteur sur une image numérisée.

Selon une version préférée de l'invention, qui permet une réalisation pratique et commode du procédé de décodage conforme à l'invention, les moyens de décomposition spectrale, d'extraction, de transformation spectrale, de sélection, d'estimation, de génération de calcul et de décision du dispositif de décodage sont incorporés dans :

- un microprocesseur,
- une mémoire morte comportant un programme pour décoder une information supplémentaire, et
- une mémoire vive comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Un moyen de stockage d'information, lisible par un ordinateur ou par un microprocesseur, intégré ou non au dispositif, éventuellement amovible, mémorise un programme mettant en œuvre le procédé de décodage d'une information supplémentaire conforme à l'invention.

La présente invention vise aussi un appareil de traitement de signal numérique comportant des moyens adaptés à mettre en œuvre le procédé d'insertion ou de décodage conforme à l'invention, ou encore comportant un dispositif d'insertion ou de décodage conforme à l'invention.

Les avantages de cet appareil de traitement sont identiques à ceux exposés ci-dessus en relation avec le procédé et le dispositif d'insertion et de décodage conforme à l'invention.

Le procédé d'insertion et le procédé de décodage peuvent plus particulièrement être mis en œuvre dans un appareil photographique numérique, une caméra numérique, un système de gestion de bases de

données, un ordinateur, un scanner ou encore un appareillage d'imagerie médicale, et notamment un appareil de radiographie aux rayons X.

Corrélativement, un appareil photographique numérique, une caméra numérique, un système de gestion de bases de données, un ordinateur, un scanner ou un appareillage d'imagerie médicale, tel qu'un appareil de radiographie aux rayons X comportent un dispositif d'insertion et/ou un dispositif de décodage conforme à l'invention.

Ces appareil photographique numérique, caméra numérique, système de gestion de bases de données, ordinateur, scanner et appareillage d'imagerie médicale présentent des avantages analogues à ceux des procédés et dispositifs d'insertion et de décodage conformes à l'invention.

D'autres particularités et avantages de l'invention apparaîtront encore dans la description ci-après.

Aux dessins annexés, donnés à titre d'exemples non limitatifs :

- 15 - la figure 1 est un schéma de principe illustrant l'insertion d'une information supplémentaire dans un signal numérique ;
- la figure 2 est un diagramme bloc illustrant un dispositif d'insertion conforme à un mode de réalisation de l'invention ;
- la figure 3 est un diagramme bloc illustrant un dispositif de traitement d'un signal numérique adapté à mettre en œuvre le procédé conforme à l'invention ;
- 20 - la figure 4 illustre schématiquement un premier mode de décomposition en sous-bande d'une image ;
- la figure 5 illustre schématiquement un second mode de décomposition en sous-bande d'une image ;
- 25 - la figure 6 est un algorithme d'insertion d'une information supplémentaire dans une image selon un mode de réalisation de l'invention ;
- la figure 7 est un diagramme bloc illustrant un dispositif de décodage conforme à un mode de réalisation de l'invention ;
- 30 - la figure 8 est un algorithme de décodage d'une information supplémentaire dans une image selon un mode de réalisation de l'invention ; et

- la figure 9 est une courbe comparative de la robustesse à la compression selon la norme JPEG d'une marque insérée par un procédé d'insertion conforme à l'invention et par un procédé de l'art antérieur.

On va décrire tout d'abord un dispositif d'insertion d'une
5 information supplémentaire dans des données numériques selon un mode de réalisation de l'invention.

Dans l'exemple ci-après, et à titre d'exemple non limitatif, les données numériques sont constituées d'une suite d'échantillons numériques représentant une image I. L'image I est par exemple représentée par une suite
10 d'octets, chaque valeur d'octet représentant un pixel de l'image I, qui peut être une image noir et blanc, à 256 niveaux de gris.

L'information supplémentaire est une marque secrète que l'on veut insérer dans l'image I de manière imperceptible et robuste. Cette marque secrète peut par exemple permettre d'identifier le créateur ou propriétaire de
15 l'image I. Cette information supplémentaire se compose dans cet exemple d'un numéro d'identification S sur un certain nombre de bits, par exemple 32 bits, associée à une clé confidentielle K, définie également sur un certain nombre de bits. Ce numéro d'identification S et cette clé confidentielle K permettront de créer, comme décrit ci-après, un signal de modulation qui sera effectivement
20 inséré dans l'image I. Une clé confidentielle K peut être associée de manière arbitraire au numéro d'identification S.

De manière générale, et comme illustré à la figure 1, un dispositif d'insertion est assimilable globalement à un codeur 1 qui code dans une image I une marque définie à partir de S et K. Une image marquée I' est fournie à la
25 sortie du codeur 1.

Cette image I' peut subir un certain nombre de traitements assimilables à l'addition d'un bruit non linéaire, tels qu'une compression et décompression, avec ou sans perte, pour être transmise ou bien stockée, ou une transformation numérique / analogique pour être visionnée, ou encore un
30 filtrage.

Après traitement, l'image I*, qui correspond à une version bruitée de l'image marquée I', peut être transmise à un décodeur 2 associé au codeur 1.

Ce décodeur 2 estimera, à partir de l'image originale I et de l'information supplémentaire S, K insérée, le signal de modulation inséré W^* dans l'image bruitée I^* . Ce signal de modulation W^* dans l'image bruitée I^* sera fourni à un détecteur 3, ainsi que le signal de modulation W inséré dans l'image I, afin
 5 d'évaluer le taux de similitude entre ces deux signaux W et W^* et de vérifier ainsi l'information de droit d'auteur par exemple qui a été insérée. Ce procédé de décodage et cette mesure de corrélation sera expliquée en détail dans la suite de la description.

Conformément à l'invention, et comme illustré à la figure 2, le
 10 dispositif d'insertion 1 comporte :

- des moyens de décomposition spectrale multi-résolution 11 des données numériques représentant dans cet exemple une image I ;
- des moyens d'extraction 12 adaptés à extraire des composantes d'une sous-bande de fréquences ;
- 15 - des moyens de transformation spectrale 13 des composantes de cette sous-bande de fréquences ;
- des moyens de choix 14 pour choisir un sous-ensemble de coefficients de la transformation spectrale ;
- des moyens de modulation 15 des coefficients de ce sous-ensemble pour insérer l'information supplémentaire ;
- 20 - des moyens de transformation spectrale inverse 16 des coefficients incluant le sous-ensemble de coefficients modulés ; et
- des moyens de recomposition spectrale multi-résolution inverse 17 des données numériques afin de reconstituer une image marquée I' .

25 De préférence, les moyens de décomposition spectrale multi-résolution 11 sont adaptés à réaliser une décomposition en ondelettes discrète et sont constitués d'un circuit de décomposition en sous-bandes, ou circuit d'analyse, formé d'un ensemble de filtres d'analyse, respectivement associés à des décimateurs par deux. Ce circuit de décomposition filtre le signal d'image I
 30 selon deux directions, en sous-bandes de basses fréquences et de hautes fréquences spatiales. Le circuit comporte plusieurs blocs successifs d'analyse

pour décomposer l'image I en des sous-bandes selon plusieurs niveaux de résolution.

De manière classique, la résolution d'un signal est le nombre d'échantillons par unité de longueur utilisés pour représenter ce signal. Dans le cas d'un signal image I , la résolution d'une sous-bande est liée au nombre d'échantillons par unité de longueur utilisés pour représenter cette sous-bande horizontalement et verticalement. La résolution dépend du nombre de décimations effectuées, du facteur de décimation et de la résolution de l'image initiale.

Cette décomposition en sous-bandes est bien connue et nous rappelons ci-dessous brièvement les différentes étapes d'analyse mises en œuvre, en référence à la figure 4, dans le cas d'une image I décomposée en sous-bandes à un niveau de décomposition d égal à 3.

Un premier bloc d'analyse reçoit le signal d'image I et le filtre à travers deux filtres numériques respectivement passe-bas et passe-haut, selon une première direction, par exemple horizontale. Après passage dans des décimateurs par deux, les signaux filtrés résultants sont à leur tour filtrés par deux filtres respectivement passe-bas et passe-haut, selon une seconde direction, par exemple verticale. Chaque signal est à nouveau passé dans un décimateur par deux. On obtient alors en sortie de ce premier bloc d'analyse, quatre sous-bandes LL_1 , LH_1 , HL_1 et HH_1 de résolution la plus élevée dans la décomposition.

La sous-bande LL_1 comporte les composantes de basse fréquence selon les deux directions du signal d'image I . La sous-bande LH_1 comporte les composantes de basse fréquence selon une première direction et de haute fréquence selon une seconde direction du signal image I . La sous-bande HL_1 comporte les composantes de haute fréquence selon la première direction et les composantes de basse fréquence selon la seconde direction. Enfin, la sous-bande HH_1 comporte les composantes de haute fréquence selon les deux directions.

Un second bloc d'analyse filtre à son tour la sous-bande LL_1 pour fournir de la même manière quatre sous-bandes LL_2 , LH_2 , HL_2 et HH_2 de niveau

de résolution intermédiaire dans la décomposition. Enfin, dans cet exemple, la sous-bande LL_2 est à son tour analysée par un troisième bloc d'analyse pour fournir quatre sous-bandes LL_3 , LH_3 , HL_3 et HH_3 de résolution la plus faible dans cette décomposition.

5 On obtient ainsi 10 sous-bandes et trois niveaux de résolution. La sous-bande de plus basse fréquence LL_3 est appelée sous-bande d'approximation et les autres sous-bandes sont des sous-bandes de détail.

Bien entendu, le nombre de niveaux de résolution, et par conséquent de sous-bandes, peut être choisi différemment, et par exemple être égal à 10 quatre niveaux de résolution avec 13 sous-bandes.

Les moyens d'extraction 12 sont ensuite adaptés à choisir les composantes de la sous-bande de très basse fréquence dans la décomposition de l'image I, c'est-à-dire dans cet exemple la sous-bande d'approximation LL_3 .

15 L'insertion de la marque S sera ainsi réalisée dans la sous-bande de basse fréquence qui est généralement peu quantifiée dans les traitements de compression et décompression d'image, de sorte que la robustesse de la marque insérée aux distorsions que subit l'image est renforcée.

La Demanderesse a constaté qu'il est possible de rajouter de l'information dans la sous-bande d'approximation de manière imperceptible à 20 condition d'atteindre un niveau de résolution suffisamment faible.

Il convient alors d'ajuster le nombre d de niveaux de décomposition en fonction de la taille de l'image I. En effet, pour une image I de taille N sur N, le nombre de composantes de la sous-bande de plus basse fréquence est dans cet exemple égal à $N/2^d \times N/2^d$.

25 De préférence, le nombre d de niveaux de décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre de composantes de la sous-bande d'approximation LL_d est compris entre 8×8 et 32×32 .

30 D'après des tests, il s'avère qu'il est préférable d'avoir une sous-bande comprenant 16×16 composantes, ce qui correspond à 5 niveaux de décomposition lorsque l'image I a une taille $N = 512$.

Les composantes de la sous-bande d'approximation LL_5 sont ainsi sélectionnées pour être fournies aux moyens de transformation spectrale 13.

A titre de variante, et comme illustrée à la figure 5, les moyens de décomposition spectrale multi-résolution 11 pourrait utiliser, au lieu de la décomposition en ondelettes décrite ci-dessus, un schéma d'approximations successives pyramidal proposé par Burt et Adelson dans "The laplacian pyramid as a compact image code ", IEEE, Trans. on communications, 31(4) : 532-540, 1983. Ce schéma consiste à extraire une version basse résolution (approximation niveau 1) de l'image I considérée par filtrage passe-bas. Cette version est sous-échantillonnée d'un facteur égal à deux dans chaque direction horizontale et verticale. L'image de détail, de niveau 0, de la même taille que l'image d'origine I, est produite par la soustraction de la version basse résolution de l'image originale I. Cette soustraction de la version basse résolution s'effectue en deux étapes : on prédit dans un premier temps l'image originale à partir de la version sous-échantillonnée en effectuant une interpolation qui ramène la version sous-échantillonnée à la taille requise de l'image originale, et on procède dans un second temps à la soustraction proprement dite de cette image interpolée de l'image originale pour obtenir l'image de détail.

On peut à nouveau décomposer l'approximation de niveau 1 en une approximation de niveau 2 par filtrage et sous-échantillonnage et une image de détail de niveau 1 par soustraction de l'approximation de niveau 2 de l'approximation de niveau 1. Ce schéma peut être itéré autant de fois que nécessaire, ici deux fois, sur l'image basse résolution pour obtenir une approximation suffisamment simplifiée de l'image et permettre une insertion invisible de l'information supplémentaire dans la version d'approximation, ici de niveau 2.

De préférence, les moyens de transformation spectrale 13 sont adaptés à réaliser une transformée en cosinus discrète ou DCT (en anglais Discrete Cosine Transform).

Cette transformation DCT, utilisée classiquement dans le traitement d'image, est ici mise en œuvre de manière efficace du fait de sa restriction à

une sous-bande de petite taille de l'image I. Cette transformation DCT permet par la suite d'obtenir une répartition de la marque insérée S dans tout le domaine spatial de l'image I.

5 Les moyens de choix 14 d'un sous-ensemble de coefficients coopèrent avec un générateur 18 de nombres suivant une fonction pseudo aléatoire initialisée par le signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S à insérer.

10 Le tirage de nombres pseudo aléatoires permet de renforcer la robustesse de la marque insérée en choisissant les coefficients de la DCT à moduler de manière aléatoire. Seule la connaissance de la clé confidentielle K et de la fonction pseudo aléatoire utilisée permet de retrouver les coefficients de la DCT qui ont été modulés.

15 De même, les moyens de modulation 15 coopèrent avec le générateur 18 de valeurs de modulation générées par une fonction pseudo aléatoire initialisée par un signal numérique S représentatif de l'information supplémentaire à insérer et comportent des moyens d'addition 15 des valeurs de modulation aux coefficients du sous-ensemble choisi précédemment.

20 Les moyens de transformation spectrale inverse 16 sont dans cet exemple une transformée en cosinus discrète inverse utilisée de manière courante dans le traitement d'image.

25 De même, les moyens de recomposition spectrale 17 comportent un circuit de recomposition classique comprenant une série de filtres de synthèse associés à des multiplicateurs par deux, de sorte qu'après plusieurs niveaux de recomposition, dans cet exemple égal à 3, une image marquée I' est fournie en sortie du codeur 1.

30 De préférence, et comme illustrée à la figure 3, les moyens de décomposition spectrale 11, d'extraction 12, de transformation spectrale 13, de choix 14, de modulation 15, de transformation spectrale inverse 16 et de recomposition spectrale 17, ainsi que le générateur 18 de nombres pseudo aléatoires sont incorporés dans un microprocesseur ou ordinateur 10, une mémoire morte 102 (ROM) comportant le programme pour insérer une information supplémentaire S, et une mémoire vive 103 (RAM) comportant des

registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Bien entendu, le programme d'insertion d'une information supplémentaire pourrait être stocké dans un disque dur 108 de l'ordinateur 10.

5 Ce programme d'insertion peut également être mémorisé en totalité ou en partie sur un moyen de stockage qui est amovible et non intégré à l'ordinateur proprement dit. Ainsi, ce programme d'insertion peut être reçu et chargé dans la mémoire morte 102 ou le disque dur 108 au moyen d'un réseau de communication 113 relié à l'ordinateur par l'intermédiaire d'une interface de
10 communication 112. On peut également envisager que le chargement du programme soit réalisé par l'intermédiaire d'un lecteur de disquettes 109 adapté à lire les instructions de programme préalablement stockées sur une disquette 110. Bien entendu, les disquettes peuvent être remplacées par tout support d'information tel qu'un disque compact à mémoire figée (CD-ROM), une bande
15 magnétique ou encore une carte mémoire.

Une unité centrale 100 (CPU) permet d'exécuter les instructions du programme d'insertion. Ainsi, lors de la mise sous tension, le programme stocké dans une des mémoires non volatiles, par exemple la mémoire morte 102, est transféré dans une mémoire vive (RAM) 103 qui contiendra également les
20 variables nécessaires à la mise en œuvre du procédé d'insertion conforme à l'invention.

La mémoire vive 103 peut comporter notamment plusieurs registres pour stocker les variables modifiées au cours de l'exécution du programme. Ainsi, elle comporte à titre d'exemple un registre pour stocker la taille de la
25 sous-bande d'approximation à chaque niveau de décomposition, un registre pour stocker le nombre pseudo aléatoire tiré pour déterminer les coefficients à moduler, un registre pour stocker le sous-ensemble de coefficients DCT choisi, un registre pour stocker les valeurs de modulation et un registre pour stocker les coefficients modulés.

30 Un bus de communication 101 permet de manière classique la communication entre les différents sous-éléments de l'ordinateur.

L'ordinateur 10 possède en outre un écran 104 permettant de visualiser par exemple l'image I à marquer et de servir d'interface avec l'utilisateur qui pourra paramétrer certaines données pour la mise en œuvre du procédé d'insertion, à l'aide du clavier 114 par exemple.

5 La fourniture des données, dans lesquelles on souhaite insérer une marque secrète, par exemple pour identifier leur auteur, à l'ordinateur 10 peut être réalisée par différents périphériques et notamment une caméra numérique 107 reliée à une carte graphique, un scanner, un appareil de radiographie aux rayons X ou tout autre moyen d'acquisition ou de stockage d'images.

10 Le réseau de communication 113 peut également être adapté à fournir une image numérique à marquer. La disquette 110 peut de même contenir des données numériques.

 A titre de variante, un microphone 111 est relié à l'ordinateur 10 par l'intermédiaire d'une carte entrée-sortie 106. Les données numériques à
15 marquer seront dans cette variante un signal audio.

 Ce dispositif d'insertion peut également être incorporé dans tout type d'appareil de traitement numérique, directement dans un appareil photographique numérique ou une caméra numérique, ou encore être intégré à un système de gestion de bases de données pour marquer les données
20 numériques mémorisées ou traitées.

 On va décrire maintenant le procédé d'insertion conforme à l'invention en référence notamment à la figure 6.

 Selon l'invention, le procédé d'insertion d'une information supplémentaire S, telle qu'une marque secrète, dans des données numériques, ici une image I, comporte les étapes suivantes :
25

 a) décomposition spectrale multi-résolution E1 des données numériques I ;

 b) extraction E2 des composantes d'une sous-bande de fréquence.

 On applique ici, à titre d'exemple, le procédé d'insertion à une image
30 de taille N sur N avec $N = 512$ octets.

 La décomposition spectrale E1 est réalisée par exemple par une transformation en ondelettes discrète. Le nombre d de niveaux de

décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre n de composantes de la sous-bande d'approximation LL est compris entre 8×8 et 32×32 composantes.

On fixe ainsi une valeur de seuil T , par exemple 32×32 , et l'on compare à chaque niveau de décomposition, le nombre n de composantes de la sous-bande d'approximation LL à cette valeur de seuil T lors d'une étape de test E21.

Si le test est négatif, c'est à dire que n est supérieur à la valeur de seuil T , on décompose la sous-bande à un niveau de résolution supérieure.

Dans cet exemple, où l'image I est carrée et de taille égale à 512 octets, on utilise une décomposition en sous-bandes avec des décimateurs par deux. La taille de la sous-bande LL, également carrée, est, à chaque niveau d de décomposition, égale à $N/2^d \times N/2^d$.

En fixant une valeur de seuil T à 32×32 octets, on obtient une sous-bande LL de taille adéquate pour un niveau de décomposition d égal à 4.

A l'étape E2, on choisit par conséquent la sous-bande d'approximation LL_4 de basse fréquence.

Selon le procédé de l'invention, une transformation spectrale des composantes de la sous-bande de fréquences LL_4 est mise en œuvre à une étape E3. Cette transformation spectrale est ici une transformée en cosinus discrète ou DCT.

Cette transformation DCT est faite sur une matrice LL_4 bien plus petite que l'image originale I , ici 16 fois plus petite que l'image I . La transformation est donc beaucoup plus rapide.

Elle pourrait également être remplacée par une transformée rapide de Fourier ou FFT (en anglais Fast Fourier Transformation).

A l'étape E4, on procède conformément à l'invention au choix d'un sous-ensemble de coefficients X_k de la transformation spectrale DCT limitée à la sous-bande LL_4 . Les coefficients X_k à moduler sont ainsi choisis dans un ensemble restreint de coefficients spectraux.

On se fixe un nombre P de coefficients à moduler : par exemple, P est égal à $(N/2^d \times N/2^d)/2$ coefficients.

La composante continue (coefficient DC) est exclue de l'ensemble des coefficients à moduler.

Dans cet exemple, le sous-ensemble de coefficients est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S à insérer.

On utilise par exemple une loi uniforme $U(0,1)$ qui, à une valeur d'initialisation donnée K, associe une suite de nombres pseudo aléatoires uniformément répartis sur l'intervalle $]0,1]$. En pratique, on exclut également la valeur 1.

On fait un tirage à l'étape E81 selon cette loi uniforme U prédéterminée initialisée par K, de telle sorte que l'on obtient $b_k = U(K)$ pour k compris entre 1 et P, avec b_k compris strictement entre 0 et 1.

A chaque tirage E81, on calcule la partie entière de $b_k \times P$ qui donne un nombre entier $n_k = \text{Ent}(b_k P)$ compris entre 0 et P-1. On choisit alors de moduler le $n_k^{\text{ième}}$ coefficient parmi les coefficients modulables de la DCT qui sont lus par exemple dans un ordre de balayage en zigzag, du coin gauche supérieur au coin droit inférieur de la sous-bande LL_4 transformée. On obtient ainsi un sous-ensemble de coefficients X_k , avec k variant de 1 à P.

Bien entendu, sans clé confidentielle K, on peut choisir les P plus gros coefficients en magnitude ou encore les P premiers coefficients dans l'ordre de parcours en zigzag, toujours en excluant le coefficient DC.

Toujours selon l'invention, les coefficients X_k du sous-ensemble choisi sont modulés à l'étape E5 par addition d'une valeur de modulation générée par une fonction pseudo aléatoire dans une étape E82 initialisée par le signal numérique S représentatif de l'information supplémentaire à insérer.

On utilise à titre d'exemple une loi Gaussienne $G(0,1)$ initialisée à l'étape E8 par le signal à insérer S.

On effectue à l'étape E82 un tirage d'une valeur de modulation $w_k = G(S)$ pour chaque coefficient X_k , avec k variant entre 1 et P.

Un coefficient de correction α est calculé à l'étape E83. Ce coefficient α peut être constant pour tous les coefficients X_k à moduler et être

typiquement égal à 0,1. Il permet d'assurer l'invisibilité de l'information insérée S.

La modulation du coefficient X_k est obtenue par addition à l'étape E5 de la valeur de modulation :

$$5 \quad X'_k = X_k(1 + \alpha w_k)$$

Un test est effectué à l'étape E52 pour vérifier si tous les coefficients X_k du sous-ensemble choisi ont été modulés.

Dans la négative, on considère le coefficient X_{k+1} suivant et on réitère le procédé à partir de l'étape E51 par tirage d'une nouvelle valeur de modulation w_{k+1} .

Lorsque le balayage est terminé, on procède à une transformation spectrale inverse à l'étape E6, ici une DCT inverse, des coefficients de la sous-bande LL_4 incluant le sous-ensemble de coefficients modulés X'_k .

Puis, une dernière étape de recomposition spectrale multi-résolution inverse E7, par utilisation de filtres de synthèse lorsqu'il s'agit comme ici d'une transformation en ondelettes inverse, permet d'obtenir l'image I' marquée.

Grâce au procédé d'insertion conforme à l'invention, la marque insérée S dans l'image I' est bien plus robuste aux traitements ultérieurs de l'image I' . Elle est répartie dans tout le domaine spatial de l'image I' , mais la modulation insérée est limitée à une bande de fréquences.

Le décodage d'une marque insérée va maintenant être décrit en référence aux figures 7 et 8.

Le décodeur 2 (voir figure 1) reçoit une image bruitée I^* et il dispose également de l'image originale I ainsi que de l'information S associée à la clé confidentielle K.

Comme illustrée à la figure 7, le dispositif de décodage conforme à l'invention comporte :

- des moyens de décomposition spectrale multi-résolution 21 des données numériques marquées I^* et des données numériques initiales I ;
- des moyens d'extraction 22 des composantes d'une sous-bande de fréquences LL respectivement dans les données numériques marquées I^* et initiales I ;

- des moyens de transformation spectrale 23 des composantes de la sous-bande de fréquence LL des données numériques marquées I^* et des données numériques initiales I ;
- des moyens de sélection 24 du sous-ensemble de coefficients
5 choisi à l'étape de choix E4 dudit procédé d'insertion dans les données numériques marquées I^* et les données numériques initiales I ;
- des moyens d'estimation 25, par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées I^* et des coefficients dudit sous-ensemble des données numériques initiales I , d'une
10 séquence estimée W^* de valeurs de modulation ;
- des moyens de génération 26 d'une séquence présumposée W de valeurs de modulation insérées à l'étape de modulation E5 dudit procédé d'insertion ;
- des moyens de calcul 28 d'une mesure de corrélation entre la
15 séquence estimée W^* et la séquence présumposée W ; et
- des moyens de décision 29 de la similitude ou non de la séquence estimée W^* et de la séquence présumposée W en fonction de ladite mesure de corrélation.

De manière analogue au dispositif d'insertion, que les moyens
20 d'extraction 22 sont adaptés à choisir les composantes de la sous-bande de plus basse fréquence LL.

Dans cet exemple, les moyens de décomposition spectrale multi-résolution 21 sont adaptés à réaliser une transformation en ondelettes discrète, les moyens d'extraction 22 étant adaptés à choisir les composantes de la sous-
25 bande d'approximation LL. Cette décomposition spectrale a été décrite en détails ci-dessus et elle est mise en œuvre par le dispositif de décodage de la même manière que dans le dispositif d'insertion décrit précédemment.

Bien entendu, si une décomposition spectrale du type pyramidale est mise en œuvre par le dispositif d'insertion, le dispositif de décodage associé
30 utilisera également le même type de décomposition pyramidale pour décoder l'information supplémentaire insérée.

De même, les moyens de transformation spectrale 23 sont adaptés à réaliser une transformée en cosinus discrète.

On comprendra aisément que, d'une manière générale, les moyens de décomposition spectrale 21, d'extraction 22 et de transformation spectrale 23 sont identiques aux moyens de décomposition spectrale 11, d'extraction 12 et de transformation spectrale 13 mis en œuvre dans le dispositif d'insertion pour l'insertion de l'information supplémentaire S que l'on souhaite décoder.

Les moyens de génération 26 de la séquence présumée W de valeurs de modulation coopèrent avec un générateur 27 de valeurs de modulation générées par une fonction pseudo aléatoire initialisée par un signal numérique S représentatif de l'information supplémentaire à décoder.

Ce générateur 27 est identique au générateur utilisé dans le dispositif d'insertion et permet de recalculer les valeurs de modulation w_k en utilisant la même fonction pseudo aléatoire.

De même, les moyens de sélection 24 coopèrent avec un générateur 27 de nombres b_k suivant une fonction pseudo aléatoire initialisée par un signal numérique K représentatif d'une clé confidentielle associée à l'information supplémentaire S à décoder.

Les moyens de décomposition spectrale 21, d'extraction 22, de transformation spectrale 23, de sélection 24, d'estimation 25, de génération 26, de calcul 28 et de décision 29 peuvent être incorporés dans un microprocesseur 10 tel qu'illustré à la figure 3. Ce microprocesseur 10 est identique dans sa structure à celui décrit précédemment pour l'incorporation du dispositif d'insertion.

Une mémoire morte 102 comporte un programme pour décoder une information supplémentaire S et une mémoire vive 103 comporte des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

Le programme de décodage d'une information supplémentaire pourrait être stocké dans un disque dur 108 de l'ordinateur 10 ou être mémorisé en totalité ou en partie sur un moyen de stockage qui est amovible et non intégré à l'ordinateur proprement dit.

Une unité centrale 100 (CPU) permet d'exécuter les instructions du programme de décodage.

La mémoire vive 103 peut comporter notamment plusieurs registres pour stocker les variables modifiées au cours de l'exécution du programme.

5 Ainsi, elle comporte à titre d'exemple un registre pour stocker la taille de la sous-bande d'approximation à chaque niveau de décomposition, un registre pour stocker les coefficients de la transformation DCT suivant un ordre de balayage prédéterminé, un registre pour stocker le nombre pseudo aléatoire tiré pour déterminer les coefficients modulés, un registre pour stocker la séquence
10 estimée de valeurs de modulation, un registre pour stocker la séquence présumée de valeurs de modulation et un registre pour stocker le calcul de la mesure de corrélation.

La fourniture des données dans lesquelles on souhaite décoder une marque secrète, par exemple pour identifier leur auteur, à l'ordinateur 10 peut
15 être réalisée par différents périphériques et notamment une caméra numérique 107 reliée à une carte graphique, ou encore un scanner, un appareil de radiographie aux rayons X ou tout autre moyen d'acquisition ou de stockage d'image.

Ce dispositif de décodage peut également être incorporé dans tout
20 type d'appareil de traitement numérique, directement dans un appareil photographique numérique ou une caméra numérique, ou encore être intégré à un système de gestion de bases de données pour décoder les données mémorisées ou traitées.

On va décrire à présent de manière plus détaillée le procédé de
25 décodage conforme à l'invention permettant de décoder une information supplémentaire S insérée dans des données numériques I suivant le procédé d'insertion conforme à l'invention.

Ce procédé de décodage comporte en référence à la figure 8 les étapes suivantes :

30 - décomposition spectrale multi-résolution E10 des données numériques marquées I* et des données numériques initiales I ;

- extraction E11 des composantes d'une sous-bande de fréquences LL respectivement dans les données numériques marquées I^* et initiales I ;

5 - transformation spectrale E12 des composantes de la sous-bande de fréquence LL des données numériques marquées I^* et des données numériques initiales I ;

- sélection E13 du sous-ensemble de coefficients choisi à l'étape de choix E4 dudit procédé d'insertion dans les données numériques marquées I^* et les données numériques initiales I ;

10 - estimation E14, par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées I^* et des coefficients dudit sous-ensemble des données numériques initiales I , d'une séquence estimée W^* de valeurs de modulation ;

15 - génération E15 d'une séquence présumposée W de valeurs de modulation insérées à l'étape de modulation E5 dudit procédé d'insertion ;

- calcul E16 d'une mesure de corrélation entre la séquence estimée W^* et la séquence présumposée W ; et

- décision E17 de la similitude ou non de la séquence estimée W^* et de la séquence présumposée W en fonction de ladite mesure de corrélation.

20 Comme dans le procédé d'insertion associé, à l'étape de décomposition spectrale E10, la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction E11, on choisit les composantes de la sous-bande d'approximation LL de plus basse fréquence.

25 A chaque niveau de décomposition, on vérifie dans une étape de test E111 si la taille de la sous-bande d'approximation est inférieure à une valeur de seuil T , et dans la négative, on réitère la décomposition spectrale à un niveau de décomposition supérieur. La valeur de seuil utilisée T est identique à celle utilisée dans le procédé d'insertion.

30 La transformation spectrale est également une transformée en cosinus discrète DCT.

A l'étape de sélection E13, le sous-ensemble de coefficients est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à décoder.

5 On utilise une loi uniforme U identique à celle utilisée lors du procédé d'insertion et initialisée par la clé confidentielle K afin de retrouver la même suite de nombres réels pseudo aléatoires. On peut ainsi retrouver l'ensemble des coefficients X'_k^* modulés dans l'image bruitée I^* et les coefficients initiaux X_k qui ont été modulés dans l'image initiale I .

10 Plus précisément, et comme décrit en détail dans le procédé d'insertion, on effectue un tirage à l'étape E131 d'un nombre $b_k = U(K)$ et on calcule la partie entière de $b_k \times P$, avec P égal au nombre coefficients modulés. On obtient $n_k = \text{Ent}(b_k \times P)$ et on sélectionne le $n_k^{\text{ième}}$ coefficient dans l'ordre de balayage prédéfini des coefficients de la DCT à la fois pour l'image bruitée I^* et
15 pour l'image initiale I .

Pour le sous-ensemble de coefficients sélectionnés, on effectue à l'étape d'estimation E14, la différence entre ces coefficients X'_k^* et X_k pour obtenir une estimation w_k^* des valeurs de modulation w_k , avec k variant de 1 à P, suivant la formule de démodulation suivante :

20
$$w_k^* = \frac{1}{\alpha} \left(\frac{X'_k^* - X_k}{X_k} \right)$$

Dans le cas où l'image I a subi d'importantes distorsions et si le coefficient modulé X_k est de faible amplitude, la valeur estimée w_k^* peut être très grande, donc aberrante. En pratique, il convient de restreindre cette valeur w_k^* : par exemple, si w_k^* est supérieure à un seuil fixé à 5, alors on attribue la
25 valeur 1 à w_k^* .

On obtient ainsi une séquence W^* correspondant à la suite des valeurs estimées w_k^* , pour k variant entre 1 et P.

A l'étape de génération E15, la séquence présumposée W de valeurs de modulation est générée par une fonction pseudo aléatoire initialisée par un
30 signal numérique S représentatif de l'information supplémentaire à décoder.

Le décodeur, disposant également de l'information S, peut en effet calculer dans l'étape de génération E15, la séquence présumée W, c'est-à-dire l'ensemble des w_k , pour k variant de 1 à P suivant la loi Gaussienne G(S) utilisée lors de l'étape de modulation E5 du procédé d'insertion.

- 5 On effectue alors dans une étape de calcul E16, une mesure de corrélation entre W et W^* , par exemple en utilisant une mesure de corrélation normalisée :

$$\text{corr}(W, W^*) = \frac{(W, W^*)}{\|W\| \times \|W^*\|}$$

$$\text{où } (W, W^*) = \sum_k w_k w_k^* \text{ et } \|W\| = \sqrt{(W, W)}.$$

- 10 Le calcul d'un taux de ressemblance par $100 \times \text{corr}(W, W^*)$ permet de décider dans une étape E17 de la similitude ou non des deux séquences W et W^* .

- Au-dessus de 50%, la corrélation est considérée suffisante pour donner une réponse positive en sortie du détecteur 3. Bien entendu, plus la
15 corrélation est proche de 100%, plus la détection et donc la reconnaissance d'une information insérée S est fiable.

- La figure 9 compare la robustesse de l'information insérée selon le procédé d'insertion conforme à l'invention et un procédé antérieur dans lequel l'information supplémentaire est insérée en utilisant une transformation DCT
20 appliquée à toute l'image I.

Cette robustesse est représentée par le taux de similarité entre la marque insérée et la marque extraite après traitement de l'image I', en fonction du facteur de qualité du traitement utilisé.

- Dans cet exemple, l'image I' a subi un traitement de compression et
25 décompression selon la norme JPEG (Joint Photographic Expert Group) à base d'une transformée en cosinus discrète DCT.

Dans le procédé conforme à l'invention, le niveau de décomposition est égal à 5 et dans les deux cas, le nombre de coefficients modulés est égal à 128.

- 30 On constate ici que le procédé conforme à l'invention donne un taux de ressemblance de 90% jusqu'à un facteur de qualité de 5, ce qui correspond

à une image fortement dégradée, alors que le procédé de la technique antérieure est nettement en dessous jusqu'à un facteur de qualité de 60.

Le procédé d'insertion conforme à l'invention et le dispositif associé permettent ainsi d'accroître fortement la robustesse d'une information insérée
5 dans des données numériques de manière imperceptible.

Bien entendu, l'invention n'est pas limitée aux exemples décrits ci-dessus, et de nombreuses modifications peuvent être apportées à celui-ci sans sortir du cadre de l'invention.

Ainsi, les données numériques marquées pourraient également être
10 des données audio.

En outre, la transformation spectrale pourrait être appliquée à une sous-bande de détail plutôt qu'à la sous-bande d'approximation de la décomposition spectrale multi-résolution.

REVENDEICATIONS

1. Procédé d'insertion d'une information supplémentaire (S), telle qu'une marque secrète, dans des données numériques (I), caractérisé en ce qu'il comporte les étapes suivantes :
- décomposition spectrale multi-résolution (E1) des données numériques (I) ;
 - extraction (E2) des composantes d'une sous-bande de fréquences (LL) ;
 - transformation spectrale (E3) des composantes de ladite sous-bande de fréquences (LL) ;
 - choix (E4) d'un sous-ensemble de coefficients (X_k) de ladite transformation spectrale ;
 - modulation (E5) des coefficients (X_k) dudit sous-ensemble pour insérer l'information supplémentaire (S) ;
 - transformation spectrale inverse (E6) des coefficients incluant le sous-ensemble de coefficients modulés (X'_k) ; et
 - recomposition spectrale multi-résolution inverse (E7) des données numériques marquées (I').
2. Procédé d'insertion conforme à la revendication 1, caractérisé en ce que lors de l'étape d'extraction (E2), on choisit les composantes de la sous-bande de plus basse fréquence (LL).
3. Procédé d'insertion conforme à l'une des revendications 1 ou 2, caractérisé en ce qu'à l'étape de décomposition spectrale (E1), la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction (E2), on choisit les composantes de la sous-bande d'approximation (LL).
4. Procédé d'insertion conforme à la revendication 3, caractérisé en ce que le niveau de décomposition par la transformation en ondelettes est prédéterminé de telle sorte que le nombre (n) de composantes de la sous-bande d'approximation (LL) est compris entre 8x8 et 32x32.

5. Procédé d'insertion conforme à l'une des revendications 1 à 4, caractérisé en ce que la transformation spectrale est une transformée en cosinus discrète.

6. Procédé d'insertion conforme à l'une des revendications 1 à 5, caractérisé en ce qu'à l'étape de modulation (E5), les coefficients (X_k) dudit sous-ensemble sont modulés par addition d'une valeur de modulation (w_k) générée par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à insérer.

7. Procédé d'insertion conforme à l'une des revendications 1 à 6, caractérisé en ce qu'à l'étape de choix (E4), le sous-ensemble de coefficients (X_k) est choisi suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à insérer.

8. Dispositif d'insertion d'une information supplémentaire (S), telle qu'une marque secrète, dans des données numériques (I), caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution (11) des données numériques (I) ;
- des moyens d'extraction (12) adaptés à extraire des composantes d'une sous-bande de fréquences (LL) ;
- des moyens de transformation spectrale (13) des composantes de ladite sous-bande de fréquences (LL) ;
- des moyens de choix (14) pour choisir un sous-ensemble de coefficients (X_k) de ladite transformation spectrale ;
- des moyens de modulation (15) des coefficients (X_k) dudit sous-ensemble pour insérer l'information supplémentaire (S) ;
- des moyens de transformation spectrale inverse (16) des coefficients incluant le sous-ensemble de coefficients modulés (X'_k) ; et
- des moyens de recomposition spectrale multi-résolution inverse (17) des données numériques marquées (I').

9. Dispositif d'insertion conforme à la revendication 8, caractérisé en ce que les moyens d'extraction (12) pour extraire une sous-bande de

fréquences sont adaptés à choisir les composantes de la sous-bande de plus basse fréquence (LL).

10. Dispositif d'insertion conforme à l'une des revendications 8 ou 9, caractérisé en ce que les moyens de décomposition spectrale multi-résolution (11) sont adaptés à réaliser une transformation en ondelettes discrète, les
5 moyens d'extraction (12) étant adaptés à choisir les composantes de la sous-bande d'approximation (LL).

11. Dispositif d'insertion conforme à la revendication 10, caractérisé en ce que le nombre de décomposition (d) par la transformation en ondelettes
10 est prédéterminé de telle sorte que le nombre (n) de composantes de la sous-bande d'approximation (LL) est compris entre 8×8 et 32×32 .

12. Dispositif d'insertion conforme à l'une des revendications 8 à 11, caractérisé en ce que les moyens de transformation spectrale (13) sont adaptés à réaliser une transformée en cosinus discrète.

13. Dispositif d'insertion conforme à l'une des revendications 8 à 12, caractérisé en ce que les moyens de modulation (15) coopèrent avec un générateur (18) de valeurs de modulation (w_k) générées par une fonction pseudo aléatoire initialisée par un signal numérique (S) représentatif de
15 l'information supplémentaire à insérer et comportent des moyens d'addition (15)
20 des valeurs de modulation (w_k) aux coefficients (X_k) dudit sous-ensemble.

14. Dispositif d'insertion conforme à l'une des revendications 8 à 13, caractérisé en ce que les moyens de choix (14) pour choisir un sous-ensemble de coefficients (X_k) coopèrent avec un générateur (18) de nombres (b_k) suivant une fonction pseudo aléatoire initialisée par un signal numérique (K)
25 représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à insérer.

15. Dispositif d'insertion conforme à l'une des revendications 8 à 14, caractérisé en ce que les moyens de décomposition spectrale (11), d'extraction (12), de transformation spectrale (13), de choix (14), de modulation (15), de
30 transformation spectrale inverse (16) et de recombinaison spectrale (17) sont incorporés dans :

- un microprocesseur (10) ;

- une mémoire morte (102) comportant un programme pour insérer une information supplémentaire (S) ; et

- une mémoire vive (103) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

5 16. Procédé de décodage dans des données numériques marquées (I*) d'une information supplémentaire (S), telle qu'une marque secrète, insérée dans des données numériques initiales (I) selon un procédé d'insertion conforme à l'une des revendications 1 à 7, caractérisé en ce qu'il comporte les étapes suivantes :

10 - décomposition spectrale multi-résolution (E10) des données numériques marquées (I*) et des données numériques initiales (I) ;

- extraction (E11) des composantes d'une sous-bande de fréquences (LL) respectivement dans les données numériques marquées (I*) et initiales (I) ;

15 - transformation spectrale (E12) des composantes de la sous-bande de fréquence (LL) des données numériques marquées (I*) et des données numériques initiales (I) ;

- sélection (E13) du sous-ensemble de coefficients choisi à l'étape de choix (E4) dudit procédé d'insertion dans les données numériques marquées (I*) et les données numériques initiales (I) ;

20

- estimation (E14), par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées (I*) et des coefficients dudit sous-ensemble des données numériques initiales (I), d'une séquence estimée (W*) de valeurs de modulation ;

25 - génération (E15) d'une séquence présumposée (W) de valeurs de modulation insérées à l'étape de modulation (E5) dudit procédé d'insertion ;

- calcul (E16) d'une mesure de corrélation entre la séquence estimée (W*) et la séquence présumposée (W) ; et

30 - décision (E17) de la similitude ou non de la séquence estimée (W*) et de la séquence présumposée (W) en fonction de ladite mesure de corrélation.

17. Procédé de décodage conforme à la revendication 16, caractérisé en ce que lors de l'étape d'extraction (E11), on choisit les composantes de la sous-bande de plus basse fréquence (LL).

5 18. Procédé de décodage conforme à l'une des revendications 16 ou 17, caractérisé en ce qu'à l'étape de décomposition spectrale (E10), la décomposition spectrale est réalisée par une transformation en ondelettes discrète, et à l'étape d'extraction (E11), on choisit les composantes de la sous-bande d'approximation (LL).

10 19. Procédé de décodage conforme à l'une des revendications 16 à 18, caractérisé en ce que la transformation spectrale est une transformée en cosinus discrète.

20. Procédé de décodage conforme à l'une des revendications 16 à 19, caractérisé en ce qu'à l'étape de génération (E15), la séquence présumée (W) de valeurs de modulation est générée par une fonction
15 pseudo aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à décoder.

21. Procédé de décodage conforme à l'une des revendications 16 à 20, caractérisé en ce qu'à l'étape de sélection (E13), le sous-ensemble de coefficients est choisi suivant une fonction pseudo aléatoire initialisée par un
20 signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à décoder.

22. Dispositif de décodage dans des données numériques marquées (I*) d'une information supplémentaire (S), telle qu'une marque secrète, insérée dans des données numériques initiales (I) selon un procédé d'insertion
25 conforme à l'une des revendications 1 à 7, caractérisé en ce qu'il comporte :

- des moyens de décomposition spectrale multi-résolution (21) des données numériques marquées (I*) et des données numériques initiales (I) ;
- des moyens d'extraction (22) des composantes d'une sous-bande de fréquences (LL) respectivement dans les données numériques marquées (I*)
30 et initiales (I) ;

- des moyens de transformation spectrale (23) des composantes de la sous-bande de fréquence (LL) des données numériques marquées (I^*) et des données numériques initiales (I) ;
 - des moyens de sélection (24) du sous-ensemble de coefficients choisi à l'étape de choix (E4) dudit procédé d'insertion dans les données numériques marquées (I^*) et les données numériques initiales (I) ;
 - des moyens d'estimation (25), par soustraction respectivement des coefficients dudit sous-ensemble des données numériques marquées (I^*) et des coefficients dudit sous-ensemble des données numériques initiales (I), d'une séquence estimée (W^*) de valeurs de modulation ;
 - des moyens de génération (26) d'une séquence présumposée (W) de valeurs de modulation insérées à l'étape de modulation (E5) dudit procédé d'insertion ;
 - des moyens de calcul (28) d'une mesure de corrélation entre la séquence estimée (W^*) et la séquence présumposée (W) ; et
 - des moyens de décision (29) de la similitude ou non de la séquence estimée (W^*) et de la séquence présumposée (W) en fonction de ladite mesure de corrélation.
23. Dispositif de décodage conforme à la revendication 22, caractérisé en ce que les moyens d'extraction (22) sont adaptés à choisir les composantes de la sous-bande de plus basse fréquence (LL).
24. Dispositif de décodage conforme à l'une des revendications 22 ou 23, caractérisé en ce que les moyens de décomposition spectrale multi-résolution (21) sont adaptés à réaliser une transformation en ondelettes discrète, les moyens d'extraction (22) étant adaptés à choisir les composantes de la sous-bande d'approximation (LL).
25. Dispositif de décodage conforme à l'une des revendications 22 à 24, caractérisé en ce que les moyens de transformation spectrale (23) sont adaptés à réaliser une transformée en cosinus discrète.
26. Dispositif de décodage conforme à l'une des revendications 22 à 25, caractérisé en ce que les moyens de génération (26) coopèrent avec un générateur (27) de valeurs de modulation générées par une fonction pseudo

aléatoire initialisée par un signal numérique (S) représentatif de l'information supplémentaire à décoder.

27. Dispositif de décodage conforme à l'une des revendications 22 à 26, caractérisé en ce que les moyens de sélection (24) coopèrent avec un
5 générateur (27) de nombres (b_k) suivant une fonction pseudo aléatoire initialisée par un signal numérique (K) représentatif d'une clé confidentielle associée à l'information supplémentaire (S) à décoder.

28. Dispositif de décodage conforme à l'une des revendications 22 à 27, caractérisé en ce que les moyens de décomposition spectrale (21),
10 d'extraction (22), de transformation spectrale (23), de sélection (24), d'estimation (25), de génération (26), de calcul (28) et de décision (29) sont incorporés dans :

- un microprocesseur (10) ;
- une mémoire morte (102) comportant un programme pour
15 décoder une information supplémentaire (S) ; et
- une mémoire vive (103) comportant des registres adaptés à enregistrer des variables modifiées au cours de l'exécution du programme.

29. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion
20 conforme à l'une des revendications 1 à 7.

30. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

31. Appareil de traitement de signal numérique, caractérisé en ce
25 qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

32. Appareil de traitement de signal numérique, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

30 33. Appareil photographique numérique, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

34.Appareil photographique numérique, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

5 35.Appareil photographique numérique, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

36.Appareil photographique numérique, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

10 37.Caméra numérique, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

38.Caméra numérique, caractérisée en ce qu'elle comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

15 39.Caméra numérique, caractérisée en ce qu'elle comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

40.Caméra numérique, caractérisée en ce qu'elle comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

20 41.Système de gestion de bases de données, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

42.Système de gestion de bases de données, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

25 43.Système de gestion de bases de données, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

44.Système de gestion de bases de données, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

30 45.Ordinateur, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

46. Ordinateur, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

47. Ordinateur, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

48. Ordinateur, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

49. Scanner, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

50. Scanner, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

51. Scanner, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

52. Scanner, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

53. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé d'insertion conforme à l'une des revendications 1 à 7.

54. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte un dispositif d'insertion conforme à l'une des revendications 8 à 15.

55. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte des moyens adaptés à mettre en œuvre le procédé de décodage conforme à l'une des revendications 16 à 21.

56. Appareillage d'imagerie médicale, et notamment appareil de radiographie aux rayons X, caractérisé en ce qu'il comporte un dispositif de décodage conforme à l'une des revendications 22 à 28.

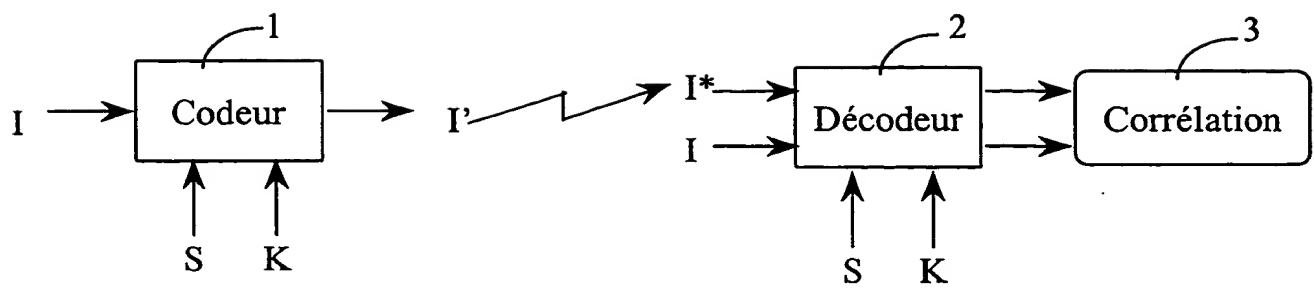


Figure 1

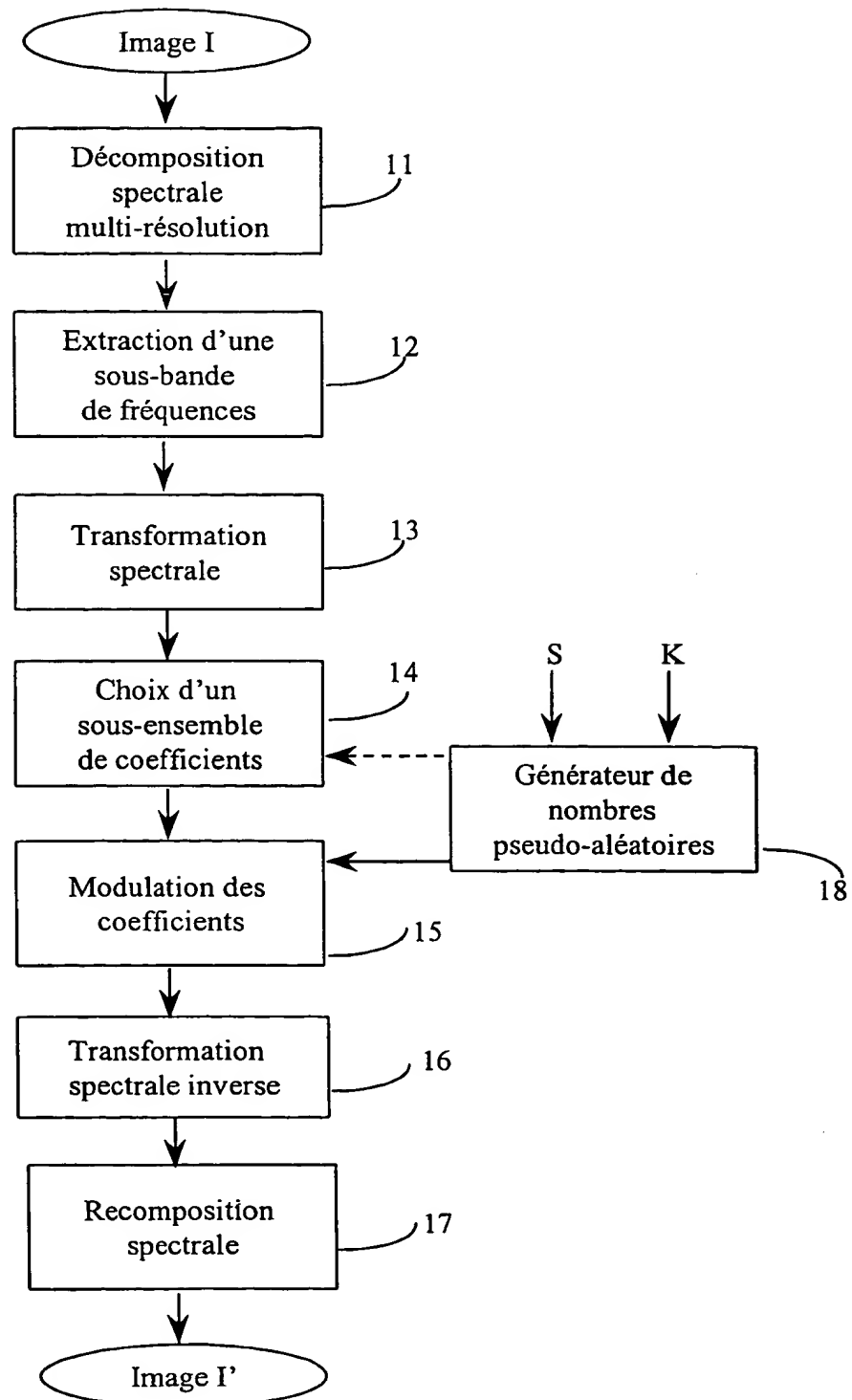


Figure 2

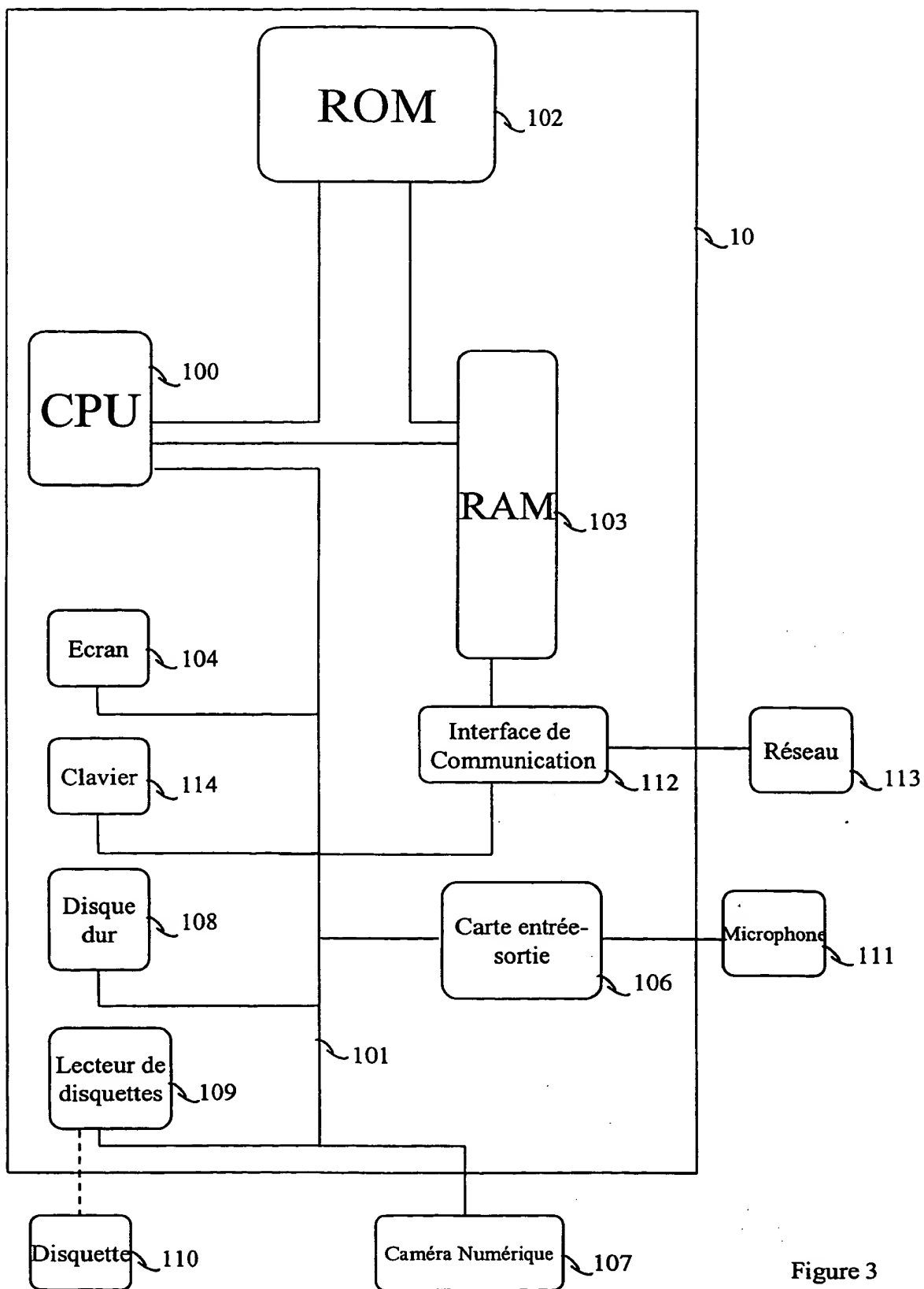


Figure 3

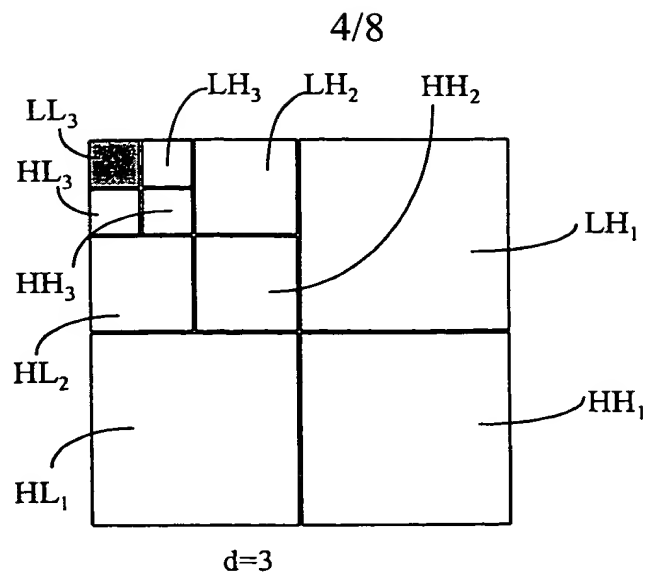


Figure 4

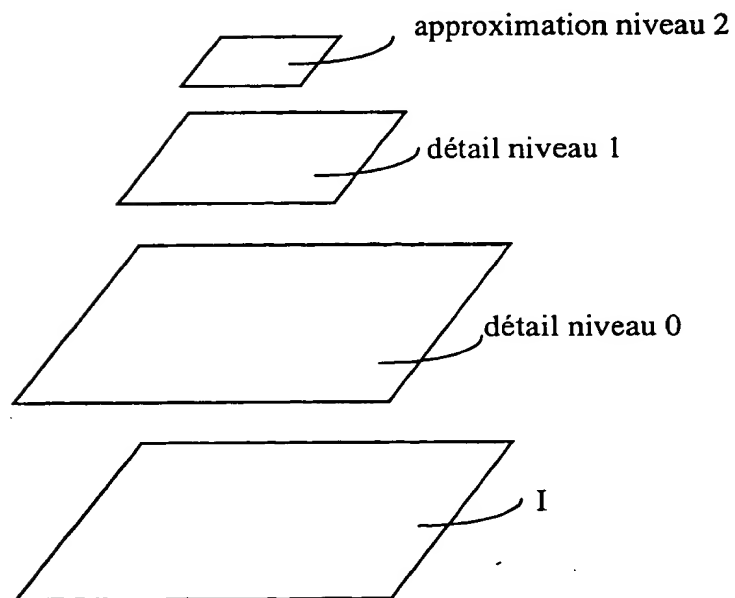


Figure 5

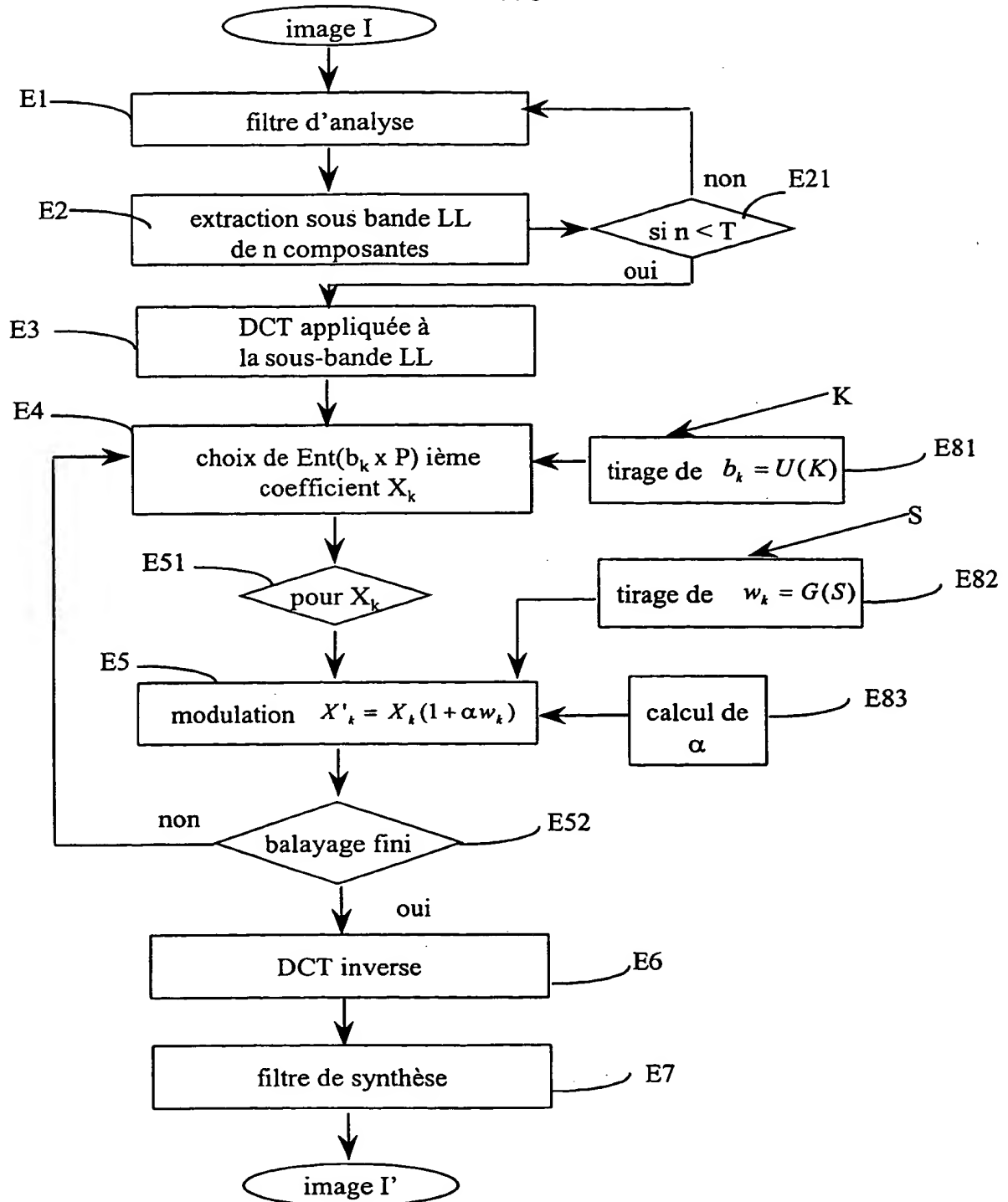


Figure 6

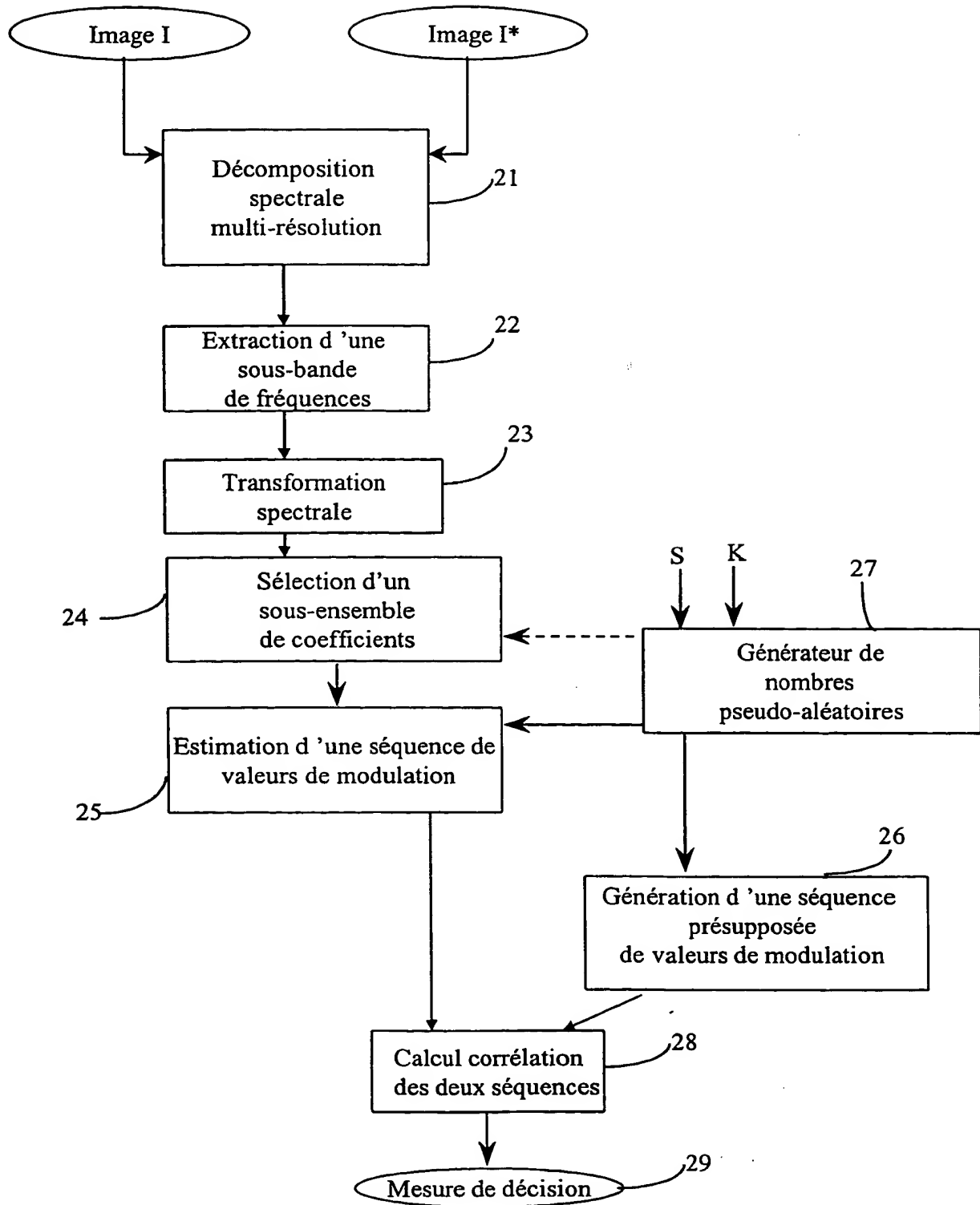


Figure 7

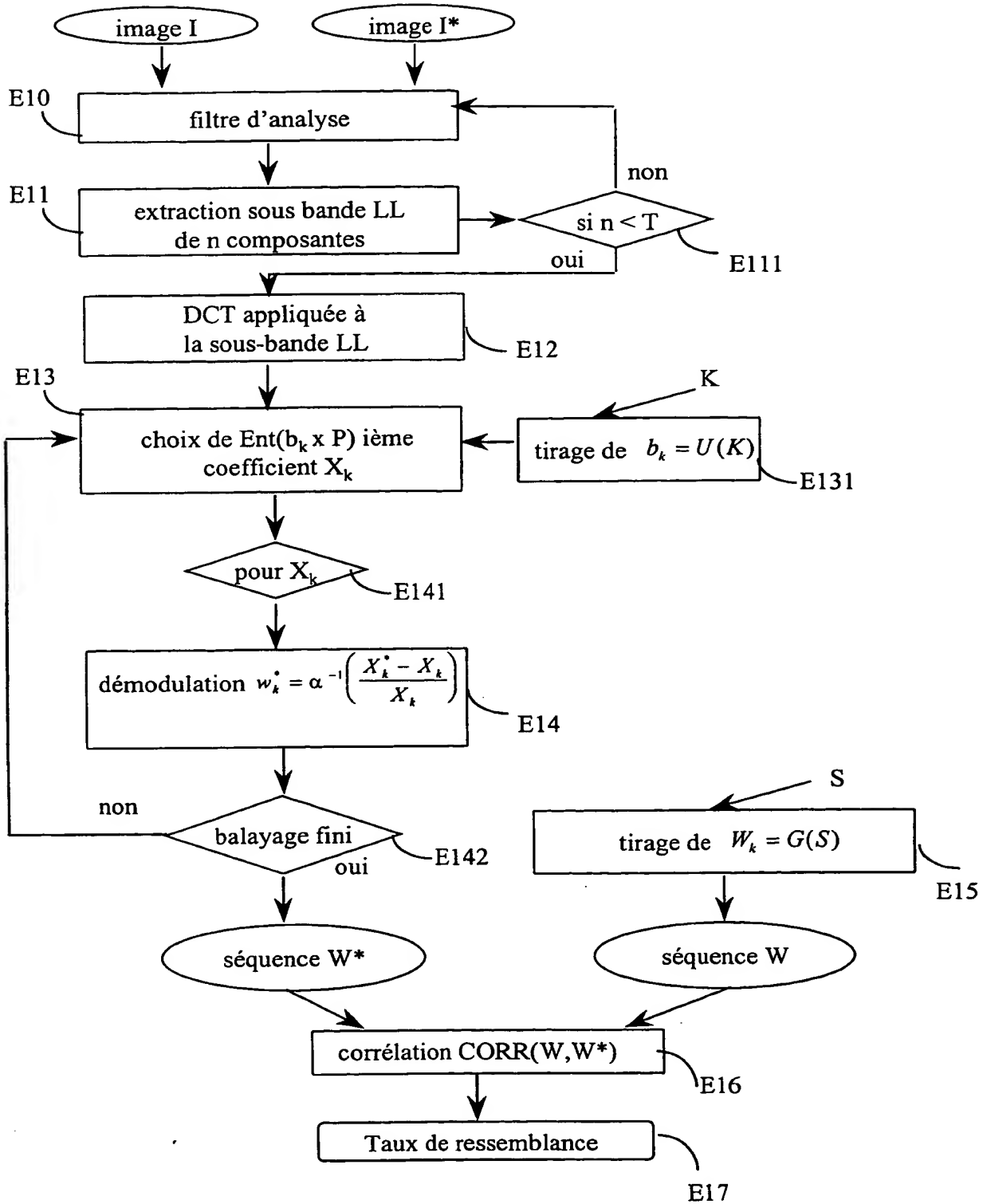


Figure 8

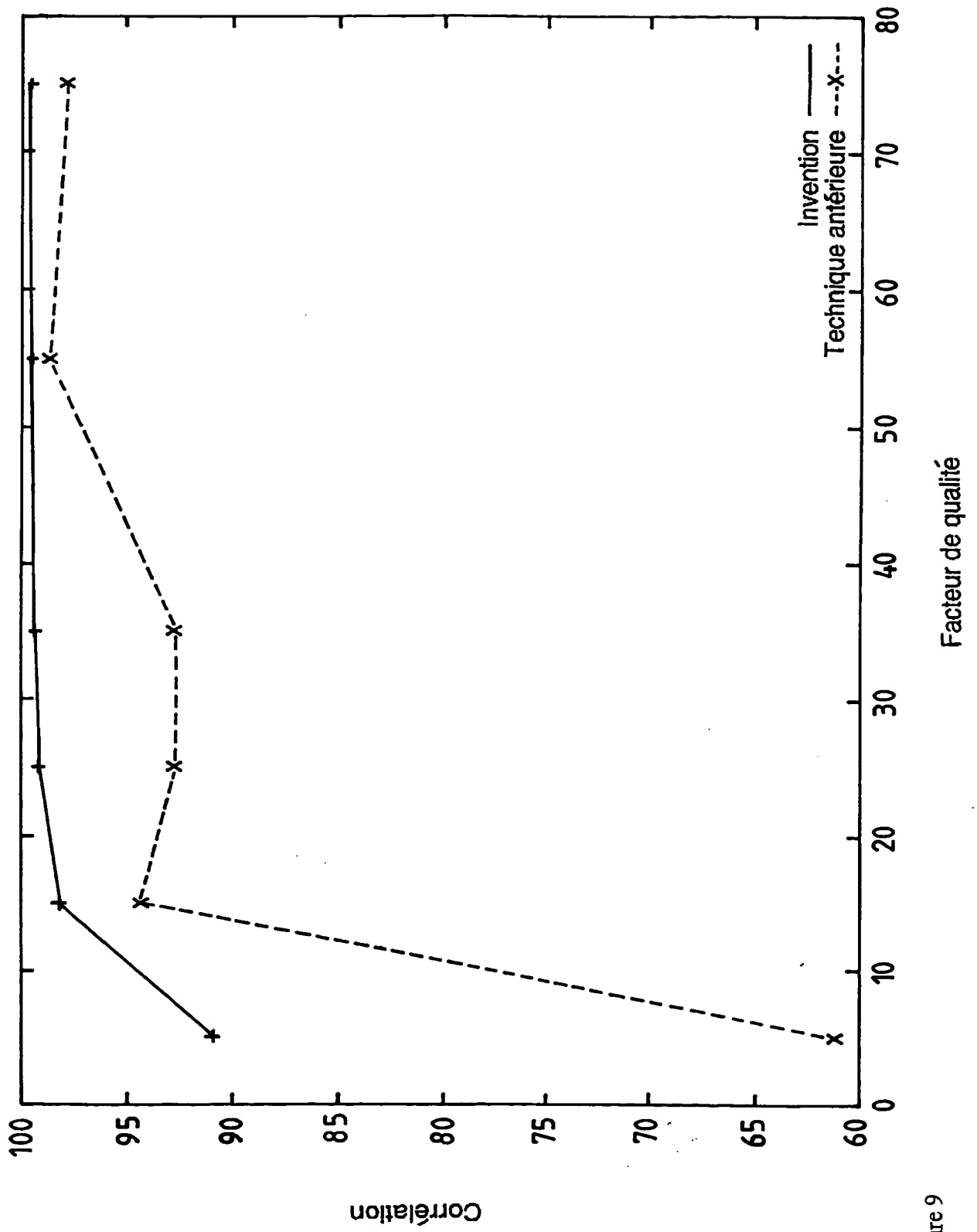


Figure 9